AOS-W 5.0.4.16

Release Notes

www.alcatel-lucent.com

26801 West Agoura Road
Calabasas, CA 91301

Contents

AOS-W 5.0.4.16 is a patch software release that fixes several previously outstanding issues. This release includes no new features.

NOTE

See Chapter 5, "Upgrade Procedures" on page 41 for instructions on how to upgrade your switch to this release.

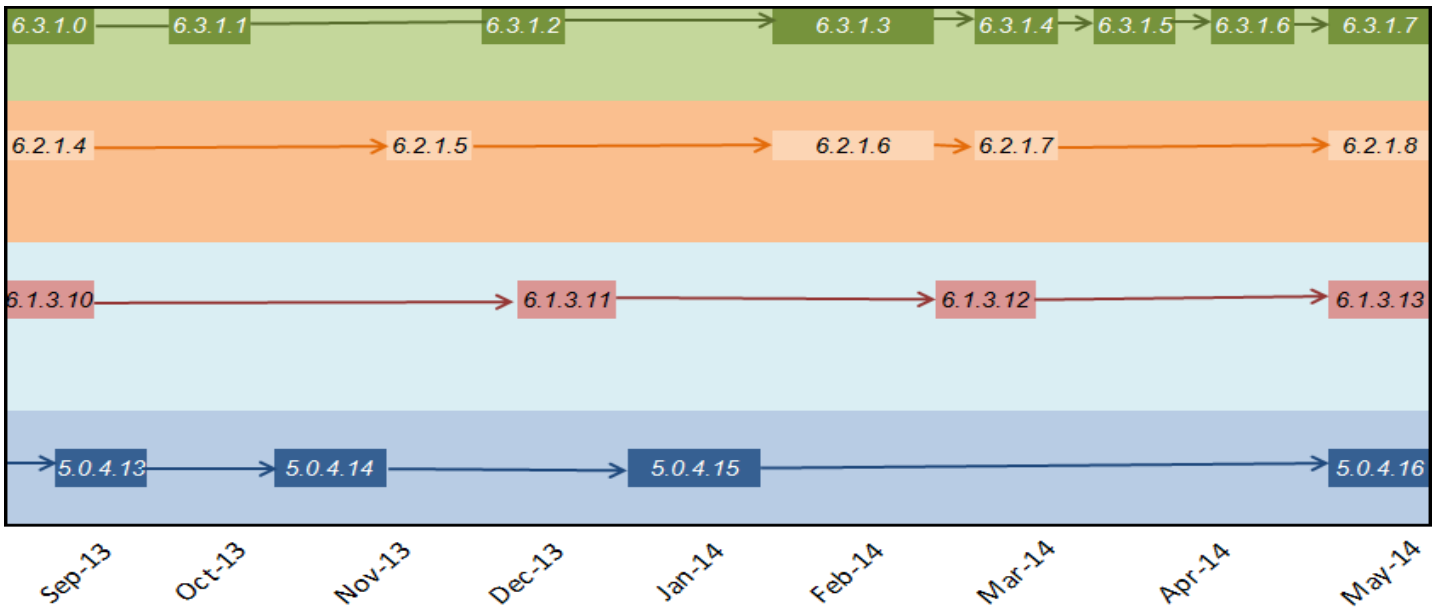
Chapter Overview

- Chapter 2, "Fixed Issues" on page 7 describes the issues that have been fixed in AOS-W 5.0.4.16 and in previous releases.
- Chapter 3, "Known Issues" on page 25 provides descriptions and workarounds for outstanding issues in AOS-W 5.0.4.16 and previous releases.
- Chapter 4, "Features in Previous Releases" on page 31 describes the features introduced in earlier releases of AOS-W 5.0.4.x.
- Chapter 5, "Upgrade Procedures" on page 41 describe the procedures for upgrading your switch to AOS-W 5.0.4.16.

Release Mapping

The following illustration shows the patches and maintenance releases included in AOS-W 5.0.4.16:

Figure 1 *AOS-W Release Mapping*



Contacting Support

Contact Center Online	
• **Main Site**	http://www.alcatel-lucent.com/enterprise
• **Support Site**	https://service.esd.alcatel-lucent.com
• **Email**	esd.support@alcatel-lucent.com
Service & Support Contact Center Telephone	
• **North America**	1-800-995-2696
• **Latin America**	1-877-919-9526
• **Europe**	+800 00200100 (Toll Free) or 1-650-385-2193
• **Asia Pacific**	+65 6240 8484
• **Worldwide**	1-818-878-4507

Chapter 2

Fixed Issues

The following issues and limitations have been fixed in AOS-W 5.0.4.16:

Table 1 *Fixed in AOS-W 5.0.4.16*

Bug ID	Description
70844 74059 76036 84403 87347 95867	**Symptom:** Firewall policies could not be deleted from the **Configuration>Security>Access control>User Roles** tab in the WebUI. Changes to the internal command syntax fixed this issue. **Scenario:** When a user edited a firewall policy from the **User Roles** tab in the WebUI, some ACL rules that contained the host keyword could not be deleted. This issue occurred because AOS-W considered single IP addresses in the source and destination to be a network value instead of a host value. This issue was found in switches running AOS-W 6.1.3.2 or later.
86032	**Symptom:** When the mobility domain was disabled, a warning message to reload the switch was displayed. This issue is fixed by making code level changes and rebooting the switch. **Scenario:** This issue was observed when data path flags are not removed after mobility domain is disabled. This issue is not limited to any specific switch model or release version.

The following issues and limitations have been fixed in AOS-W 5.0.4.15:

Table 2 *Fixed in AOS-W 5.0.4.15*

Bug ID	Description
59292 66990 66996	**Symptom:** Compile errors were produced intermittently when an AOS-W 5.0.4.x management information base (MIB) was imported to HP OpenView 9.10 or above. Updates to the SNMP MIB fixed this issue. **Scenario:** This issue occurred when a new MIB browser was used. This issue was observed in an OAW-4504 switch running AOS-W 5.0.4.x.
76021	**Symptom:** A core file from an AP with a special character in the AP name included the special character in the core file name, causing the TFTP dump server to reject the file. Removing special characters from the core file name before it sends the file to the dump server fixed this issue. **Scenario:** This issue occurred when an internal process crashed on an AP, and a core file of troubleshooting data was sent to the dump server defined in the AP's system profile. This issue was observed on APs with one or more special characters in the AP name, and was not limited to a specific AP model.
76239	**Symptom:** VPN user entries did not properly age out of the user table. These user entries became stale and prevented new users with the same IP address from associating to the network. This issue occurred when one inner-IP address was assigned to two different Layer 2 Tunneling Protocol (L2TP) outer-IP addresses. Changes that prevented a previously assigned IP address from returning to the free IP address pool during Next-pin mode using SecureID authentication fixed this issue. **Scenario:** The issue was observed on an OAW-4324 switch running AOS-W 5.0.4.5 during Next-pin mode using SecureID as authentication.
76484	**Symptom:** RADIUS authentication failed in networks that had different Maximum Transmission Unit (MTU) values. Updating the socket options to allow the switch to send RADIUS requests to the RADIUS server when EAP termination is enabled fixed this issue. **Scenario:** The RADIUS authentication failed when the MTU value in the network between the switch and RADIUS server was different. This issue was not specific to any switch model or AOS-W version.

Table 2 *Fixed in AOS-W 5.0.4.15*

Bug ID	Description
82199 91183	**Symptom:** IPv6 Access Control List (ACL) on the master switch did not synchronize with the local switch. Corrections to the format of the configuration commands associated with IPv6 ACLs under the user-role fixed this issue. **Scenario:** This issue was observed when IPv6 ACLs were configured under the user-role of the master switch. This issue was observed on switches running AOS-W 5.0.4.x.

The following issues and limitations have been fixed in AOS-W 5.0.4.13:

Table 4 *Fixed in AOS-W 5.0.4.13*

Bug ID	Description
73459 85136 86427	**Symptom**: The output of the **show acl hits** CLI command and the **Firewall Hits** information on the **UI Monitoring** page of the switch WebUI showed inconsistent information. **Scenario**: This issue occurred because the formatting of the XML response from the switch to the WebUI was incorrect, when the output was beyond the specified limit. This issue was not limited to a specific switch model or release version.
87091	**Symptom**: The **Guest Provisioning** page of the WebUI showed incorrect alignment when it was printed from Internet Explorer 8 or Internet Explorer 9 web browser. HTML style improvements resolved this issue. **Scenario**: This issue was first identified in AOS-W 5.0.4.0. This issue was not observed when users viewed the switch WebUI using older versions of Internet Explorer (version 6 and 7).
87416	**Symptom:** The default server certificate needed to be replaced because the certificate used by the switches running AOS-W 5.x was nearing the expiry date. This issue is fixed by generating an Aruba issued 1k server certificate and included in AOS-W 5.x. Now, applications such as WebUI, Captive Portal, and 802.1X can use this certificate as a default server certificate. **Scenario:** This issue was observed in AOS-W 5.x and not specific to any switch model. **Note:** Windows 7 clients reject the server certificate after 802.1X authentication. Use the following steps as a workaround: • Use custom certificate instead of the default certificate. • Download the trusted certification authority (CA) certificate from the Aruba Support Tools section and install on windows 7 clients. • Disable the server certificate validation on windows 7 clients.

The following issues and limitations have been fixed in AOS-W 5.0.4.12:

Table 5 *Fixed in AOS-W 5.0.4.12*

Bug ID	Description
56398	**Symptom**: A switch with a loopback address that was in a different subnet than any VLAN subnet, OSPF could not advertise this loopback address. The AOS-W command-line interface now includes a **router ospf redistribute loopback** command to configure OSPF to advertise a loopback address even when it is in a different subnet than any configured VLAN. **Scenario**: This issue was first identified in AOS-W 6.1.2.3, and is not specific to any switch model.

Table 5 *Fixed in AOS-W 5.0.4.12 (Continued)*

Bug ID	Description
72951	**Symptom**: An OAW-AP85 stopped responding and rebooted unexpectedly. Internal memory improvements have resolved this issue. **Scenario**: This issue was triggered by invalid memory access, and occurred on an OAW-AP85 configured with virtual APs in bridge, tunnel and decrypt-tunnel forwarding modes, where the 802.11g radio was configured as an air monitor, and the 802.11a radio was configured as a campus AP.
73381	**Symptom:** A switch became unresponsive, and required a reboot to recover. Changes to how the switch manages requests to delete and clear MAC addresses have resolved this issue. **Scenario**: This issue occurred on an OAW-S3 local switch module running AOS-W 6.1.3.4, and was triggered by a loop condition in the wired ports on a remote AP.
73381	**Symptom:** A switch became unresponsive, and required a reboot to recover. Changes to how the switch manages MAC address delete and clear requests have resolved this issue. **Scenario:** This issue occurred on a local OAW-6000 switch running AOS-W 6.1.3.4, and was triggered by a loop condition in the wired ports on a remote AP.
74010 77980	**Symptom:** The Station handoff-assist feature had issues due to the use of outdated Received Signal Strength Indication (RSSI) information. The station handoff-assist feature now uses a more accurate measurement for RSSI to avoid redundant handoffs, resolving this issue. **Scenario:** Due to the use of outdated RSSI, the output of the **show ap association** and **show ap monitor stats** command could display inaccurate data. This issue was not specific to any AP or switch model.
80419 80523	**Symptom**: A feature allowed the AOS-W DNS server to reveal its version number. This feature has been disabled in AOS-W 5.0.4.12 as a security precaution. **Scenario**: This issue was identified in AOS-W 5.0.4.11.
81865	**Symptom**: When a loopback IPwas configured on a switch but the switch IP was set to the IP address of another VLAN interface, there was no entry for the loopback interface's IP address in the user table. This issue is fixed as AOS-W now creates an entry in the user table if the switch IP address is different from the loopback IP address. **Scenario**: This issue was identified on AOS-W 6.1.3.5 and is not limited to any specific switch model.

The following issues and limitations have been fixed in AOS-W 5.0.4.11:

Table 6 *Fixed in AOS-W 5.0.4.11*

Bug ID	Description
41862 41864 41780 41267 75404 75407	**Symptom:** STM module of the switch crashed due to an internal memory leak. **Scenario:** The issue was observed when 4000 clients were connected to 220 APs and the Airwave server tried to poll the switches every 5 minutes. The issue was found in switches running AOS-W 3.4.3.2.
44646 48141 48148 49335 49550 68062	**Symptom:** The RAP MAC addresses added in the RAP whitelist were displayed in the Guest provisioning accounts. **Scenario:** The issue was observed when users logged in as guests executed the `show local-userdb-ap entries command`. The issue was found in switches running in AOS-W 5.0.x.x version.

Table 6 *Fixed in AOS-W 5.0.4.11 (Continued)*

Bug ID	Description
53078 53114	**Symptom:** The Virtual Router Redundancy Protocol (VRRP) packets were getting dropped when `bcmc-optimization` parameter was enabled on the VLAN interface, in which VRRP was configured. **Scenario:** The issue occurred on switches running AOS-W 5.0.4.10 or earlier.
54939 60800	**Symptom:** One or more APs were not listed in the SNMP table (wlanAPIpAddress). However, the APs missing from the SNMP table were active on the switch side. **Scenario:** The issue was observed in APs whose MAC address ends with FF or FE. The issue was not specific to a switch model and software version.
61351 52450	**Symptom:** Clients were connected as non HT (High-Throughput) devices when the AP's channel was changed. **Scenario:** The issue occurred on switches and the AP models running AOS-W versions 5.0.4.2 to 5.0.4.11.
62933 66701 68600 67645 71772	**Symptom:** OAW-AP124, OAW-AP125, AP-104, and OAW-AP105 crashed when sending traffic to 20 or more clients. **Scenario:** The issue occurred when switching the traffic forwarding between tunnel and de-tunnel modes. The issue was not specific to any switch model or software version.
63386	**Symptom:** The control messages between the switch and its APs contain a sequence number between 0 and 64k. In some cases, when the sequence number rolled back to 0, the message with the sequence number 0 was getting dropped. **Scenario:** This issue occurred on switches running AOS-W 5.0.x.x.
75232	**Symptom:** For large deployments, an internal system error occurred in the switch and APs failed to connect to the switch. **Scenario:** The issue was seen in large deployments where the size of the config file was more than 360 KB and there was large number of references to one profile instance. Due to this there was an internal system error and the APs were unable to connect to the switch. This issue is now fixed. It occurred in AOS-W 5.0.4.6 and is not specific to any switch.

Table 7 *Fixed in AOS-W 5.0.4.10*

Bug ID	Description
57624	**Symptom:** In previous versions of the switch software, the potential exists that the power amplifier (PA) for the 5GHz radio of the 100 Series access points is subjected to a short and unintended power spike exceeding the specified operating range of the associated components. It has been found that in some rare cases, this can lead to permanent damage to the PA, resulting in a failure of the access point .While the failure rate associated with this issue is very low, a series of changes have been implemented in software to avoid this potential risk altogether. **Scenario:** This issue occurred on AP-100OAW-100 series APs that scan outside home channels aggressively.
70327	**Symptom:** APs didn't support ETSI DFS standard EN301893. With the exception of OAW-RAP5WN and the OAW-AP120 Series APs, all supported APs will comply with version 1.6.1 or later of the when the system is upgraded to AOS-W 5.0.4.10. **Scenario:** The OAW-RAP5WN and the OAW-AP120 Series APs can be upgraded to AOS-W 5.0.4.10, but will not become compliant with the version 1.6.1 of the standard. OAW-RAP5WN and the OAW-AP120 Series APs already installed in a network are allowed to remain compliant with the previous version of the standard, but any new devices added to the network after 12/31/2012 must comply with the version 1.6.1 or later wherever ETSI rules apply.

Table 8 *Fixed in AOS-W 5.0.4.9*

Bug ID	Description
73343	Support for channels 100 - 140 has been added for OAW-AP60, OAW-AP61, OAW-AP70, and OAW-AP85 for Saudi Arabia.

Table 9 *Fixed in AOS-W 5.0.4.8*

Bug ID	Description
50850	Role derivation for bridge mode users is now properly working when machine authentication and 802.1X authentication are configured at the same time. Previously, the user was incorrectly placed in the machine authentication role even after successful machine authentication and user 802.1X authentication occurred.
52016	The error message `Save failed: Module Authentication is busy. Please try later` is no longer triggered by adding 100 user roles each with six or more session ACLs.
54412 56830 64825 69514	An issue has been fixed where the Station Management (STM) module rebooted on a switch running AOS-W 5.0.x and the clients connected to APs on the switch were not able to access resources. This issue occurred when the 802.11k feature was enabled on the APs/switch and the 802.11k enabled wireless clients sent beacon reports to the APs.
56707	The `show ap database` command no longer displays the local switch's status as down on the master, when all the APs on the local switch are up.
59708	An issue has been fixed where Apple iOS clients disconnected from the WEP and TKIP SSIDs on switches. This issue occurred due to the incorrect encryption of the LLC traffic.
61389	An issue has been fixed where the STM module crashed resulting in an AP rebootstrap. This happened occasionally when a wireless client used an association ID that was used earlier by another wireless client. This issue was observed in switches running AOS-W 5.0.4.x.
62687	An issue has been fixed where the AP LED status on a LC-2G24FP line card did not display AP activity after connecting an AP to the Fast Ethernet (FE) port of the line card. This was observed in an OAW-S-1 after upgrading the AOS-W from 3.x to 5.0.4.x.
63665	An issue has been fixed where the authentication module crashed resulting in frequent disconnection of wired and wireless clients. This happened when the aaa-profile for an associating wired or wireless client was unavailable. This issue was observed in switches running AOS-W 5.0.4.x.
64889	OAW-AP105 now supports the Uruguay (UY) regulatory domain.
67622	OAW-AP68 and OAW-AP68P now support the Egypt (EG) regulatory domain.
69140	An issue has been fixed where the GE1/0 - 1/3 port on the 650 switch did not link up and transmit packets because of an error in the static configuration of the Full duplex setting. This issue was observed in AOS-W 3.4.5.0, 5.0.2.1, 5.0.4.7, 6.0.2.1, 6.1.2.5, 6.1.3.1, 6.1.3.3 with a 650 switch.
69419	An issue has been fixed where incorrect values were written to the `wlsxWlanStationStatsTable` MIB, especially with respect to per AP user count and/or bandwidth. This issue was seen in AOS-W 5.0.3.3 with an OAW-S3 switch and a large number of OAW-AP92s operating as RAPs and deployed as hotspots. The root cause was attributed to personal hotspots on the client devices that were using the same MAC address as the client's connection to the Alcatel-Lucent AP.
69644	An issue is fixed where the BSSIDs of APs were frequently dropped from the output of `show ap monitor ap-list` command. As a result, the APs could not classify clients and create SNMP statistics. This issue was seen in AOS-W 5.0.3.3 on OAW-S3 switches with a large number of OAW-AP92s operating as RAPs. The root cause was attributed to beacon failures due to a bad RF environment.

Table 9 *Fixed in AOS-W 5.0.4.8 (Continued)*

Bug ID	Description
71027	An issue has been fixed where clients using split-tunnel forwarding mode were assigned incorrect roles on a remote AP following a change in configuration. Clients (iPads) could not log in after the configuration change. This issue was seen in AOS-W 5.0.4.7 and was attributed to the ACL/role changes not getting updated in the RAPs.

Table 10 *Fixed in AOS-W 5.0.4.7*

Bug ID	Description
40550 41623	A WebUI issue is fixed where the auto-generated guest password created using the Guest Provisioning user account contained only digits and no alphabetic characters.
41363	A WebUI issue is fixed where the APs did not come up if they were assigned to an AP group with a plus (+) sign in its name.
57229	The issue where all the External Services Interface (ESI) servers went down when one of the ESI servers was not reachable is fixed.
58599	The issue is fixed where the CLI access to the switch was unavailable when multiple `show ap debug stat` commands were run.
59390	The issue is fixed where the station management module (STM) on the switch crashed due to the memory leak has been.
60594	A process crash on APs while upgrading switches from RN 3.x to 5.x when VLANs for *backup* and *always bridge* Virtual APs were set to **all**, is fixed.
63952 66355 68121	An issue with the Guest Provisioning Page (GPP) that did not allow you to modify the existing users by clicking the **Edit** button has been fixed.
65850	The Control Plane Security module may become unresponsive if it has multiple open connections to the Profile Manager while running AOS-W 5.0.4.4 or later. This issue has been fixed.
65805 66181	The switch sends ARM messages to the AP to optimize its channel and power settings. These messages have been modified so they no longer generate log error messages if the AP does not acknowledge them. If the switch encounters a busy state, it will resend the message without waiting for an acknowledgement from the AP.
66477 66476	An issue with the APs using channels 12 and 13 which are not specified for the country code CO has been fixed.
67227 67231	An issue where the local switches reboot during verification of the ISAKMPD certificate has been fixed.
67376	An issue where an OAW-AP125 reboots with a cache error when virtual APs are deleted has been fixed.
67534 68105 68557	An issue where an OAW-AP105 stopped responding to client transmissions until the AP was rebooted has been fixed.
68712	A problem where AOS-W VIA failed to start because of an expired certificate has been corrected.

Table 11 *Fixed in AOS-W 5.0.4.6*

Bug ID	Description
47990	Backup SSID users correctly show up on the L3 user table and do not incorrectly age out.
48961	When the port status is changed to “down,” the speed/duplex configuration is no longer incorrectly removed.
51460	OAW-AP125 no longer crashes due to a kernel page fault at the virtual address.
52321 60284 62129 62594 65119	Port channels can now be enabled through the WebUI.
52770 58764 60371 60480	An unexpected switch reboot caused by an arci-cli helper crash due to a double free issue when the queried module is busy has been fixed.
53804 53004	The FPCLI does not crash on an AP name over 64 characters long while executing the `show ap debug` command.
53821 54053 55125 55130 55616 56657 59457 62102 62006 62206	The mysql process now begins before any other processes to help prevent an unexpected switch reboot that occurred following a number of module crashes.
53880	802.11n is now allowed for the Russia (RU) country code.
53897 52825 55118 53365 59274 61930	An OAW-AP125 crash caused by a node leak has been fixed.
54256 54609 57659	An AP crash due to a kernel page fault caused by a stack corruption has been fixed.
55206 59262	The commands `show user ip` or `show user mac` are no longer truncated.
55503	Server roles for wired VPN users authenticating against a RADIUS server are now derived correctly.
56756	An AP reboot caused by a kernel panic that occurs when the AP comes out of power save and the AP tries to flush the legacy PS queue.
56815 60790	An issue in which WPA2 802.1X split-tunnel users were intermittently not able to complete the connection with split-tunnel SSID until the RAP rebooted has been fixed.
56920 58957	AOS-W has been changed to reduce the number of extraneous configuration errors that appear in the log after upgrading to 5.0.4.x or later.

Table 11 *Fixed in AOS-W 5.0.4.6 (Continued)*

Bug ID	Description
57249	Client can associate as 40Mhz capable with ZA regulatory domain. Before the fix, with ZA regulatory domain client could associate only as 20Mhz capable.
57831	Improvements to the datapath module increase switch stability, and prevent the switch from failing to respond due to datapath exceptions.
57869	High CPU in STM no longer causes APs to drop from the switch when port value on the ALG netservice configuration goes beyond 65535.
57906	An AP reboot caused by a kernel panic due to a memory corruption has been fixed.
58108	An unexpected AP reboot caused by a kernel panic that occurred while radio calibration was attempted during a radio reset has been fixed.
58132 58105 58333 58334	An unexpected AP reboot has been fixed by preventing the AP from queuing new packets during a channel change.
58256	An OAW-AP105 crash with raw call trace `asap_chrdev_tx_to_am` has been fixed.
58261	An OAW-AP105 crash with a raw call trace `tlb_do_page_faults` no longer occurs.
58358	A parameter has been added under HT-SSID profile - sw-retry (type: boolean) to avoid packet drop for certain types of clients.
58380	An OAW-AP125 no longer crashes after a virtual AP is repeatedly enable and disabled.
58502	Packets are now sent from the Trunk port on the switch to a client on the trunk port behind a RAP with a proper VLAN tag.
59019	When a remote AP is behind an intermediate firewall that has been rebooted, RAPs try different src-port on each IPSec retry so the firewall will not count each retry as a part of the same, previously-denied session.
59027	A bridge user-entry now correctly ages out when a user roams to another RAP on a different management VLAN.
59227 59368 59372 59369	An AP kernel panic that occurred while a channel change or reset was in progress has been fixed.
59367	An unwanted AP reboot caused by a kernel panic at `ath_process_uapsd_trigger` message no longer occurs.
59484	Nothing is written into the HAL registers (disable or enable interrupts) if a reset/change is in progress.
59706 61804	An unwanted AP reboot caused by a kernel panic at aruba_deferred_set_channel message no longer occurs.
60273 51912	User bandwidth contracts are now deleted correctly when the corresponding user entry is deleted.
60667	Authentication improvements allow TACACS command accounting to function correctly, even in environments with up to 400milliseconds delay between the switch and the TACACS server.

Table 11 *Fixed in AOS-W 5.0.4.6 (Continued)*

Bug ID	Description
61076	IKE is now able to rekey correctly at any time.
61191	An issue has been resolved where RX frames which were not mapped to an RX descriptor could cause an AP to unexpectedly reboot.
61667	The `firewall broadcast-filter arp` command no longer causes the local switch to use the incorrect route-cache entry.
61720	The default regulatory domain profile for the country code JP3 contains all valid channels for that regulatory domain.
61921	Memory improvements increase the stability of the auth module.
62391	Improvements to RX queue access resolved an issue that could cause an AP to unexpectedly reboot.
62455	The ifIndex value returned by the IP table during an SNMP walk on a 620 switch correctly matches the MIB value returned in the ifDescr table.
62507	Oman regulatory domain channels are updated for the OAW-AP124 and OAW-AP125.
62609	APs no longer miss heartbeats and rebootstrap when connected to a Juniper MX-480.
62694	Improvements to the format of RF Plan files allow files to be imported using the RF Plan WebUI without triggering XML errors.
63502 63701	The reboot cause is now displayed correctly in the output of the command `show switchinfo`.
63771 55521	An auth crash occurring on a SC1 switch module due to a memory leak has been fixed.
65072	When STP is disabled on a switch with a redundant link, the switch now correctly floods BPDUs and one of the ports on the uplink switch moves from forwarding mode to blocking mode as expected.

Table 12 *Fixed in AOS-W 5.0.4.5*

Bug ID	Description
63808 64086	Control plane security APs and RAPs configured with a Virtual AP in bridge forwarding mode no longer experience repeated crashes due to a kernel panic. This kernel panic was caused by the code that handles client mobility in bridge mode.
64192 64302	Bandwidth contracts are now correctly applied to sessions and policing occurs.

Table 13 *Fixed in AOS-W 5.0.4.4*

Bug ID	Description
41243	After upgrading a switch, guest users are now correctly displayed as guest provisioning users just as they were prior to the upgrade.

Table 13 *Fixed in AOS-W 5.0.4.4*

Bug ID	Description
45571	Captive portal now works correctly on local switches when the guest VLAN has `ip nat inside` is enabled.
45624 53886	AOS-W has been changed so that the OAW-AP120 series AP will correctly acknowledge data frames that are preceded by a CTS frame.
50041 51681 52458 57635 61578	An unexpected hybrid mode AP crash caused by a change made to the phy-restart setting has been fixed.
51668 51619 52869 53141 53774 54568 83940 83998	Unexpected switch reboot following a datapath timeout caused by a race condition has been fixed.
52492 53600 56561 54231 57302 55620 61152 61155 56928	An unexpected switch reboot due to a hard watchdog accompanied by “reason for reboot: unknown” has been fixed. Additionally, a change has been made to AOS-W to prevent the use of “reason for reboot: unknown” for unexpected reboots. Unknown reboots were caused by flash write failures. Now, the flash write is retried by performing an erase followed by another write.
52758	An issue that occurs when the switch's SNMPD module does not respond to the AMP's SNMP requests has been fixed.
53497 56022 58185 57411 59249 61210	An unexpected switch reboot caused by an internal module crash due to a PAPI corruption has been fixed.
54343	An STM module crash due to an STM memory leak caused by voice client call session being created but not deleted after the session ends has been fixed.
54621	Heat map coverage for APs no longer incorrectly displays in a diamond shape.
57406	A RAP ASSERT occurring when a wired-split-tunnel client is unplugged and replugged 5 or more times has been fixed.
57950	An internal module crash caused by race conditions in accessing internal data structures of Alcatel Mapping Adjacency Protocol (AMAP) module has been fixed.
58540	When voip-content-enforcement is enabled, IP ToS is no longer being reset to 0 in the downstream RTP frames of the NOE voice sessions.
60431	An internal module crash that occurred when the `show trunk` command was issued on a switch with a large number of non-contiguous VLANs has been fixed.
61545	The cause: unknown pop-up message that occasionally appeared when the user clicked on the **Configuration** tab in WebUI after a reboot has been fixed.

Table 13 *Fixed in AOS-W 5.0.4.4*

Bug ID	Description
61547	An auth module crash that is suspected to be due to an AP sending invalid data in ap_name string has been fixed.
61895 61877 61896 62439	A datapath exception resulting in an unexpected switch reboot has been fixed. This datapath exception occurred when a bandwidth contract was deleted while packets were being added to its queue.
62296 62297 62501 62476 62474 62472 62469 62502 62477 62468 62089	The Alcatel-Lucent OAW-4306GW switch is no longer susceptible to continuous rebooting if its internal AP (radio) is configured in Air Monitor mode (am-mode).
62493 62398	Bcmc-optimization with RAP Wi-Fi and wired ports in tunnel-mode no longer breaks connectivity.
62865 62915	An STM module crash caused by a null pointer access problem in SCCP ALG has been fixed.

Table 14 *Fixed in AOS-W 5.0.4.3*

Bug ID	Description
56641 58232 58231	An unexpected OAW-S3 switch reboot due to a crash in the datapath module has been fixed.
53904 60036 60049 60293	A number of issues related to core dump decoding resulting in an incomplete core file have been fixed. These issues included inability to access the user table memory from the SOS core file and a race condition that caused the intent/cause data to overwrite the SOS core dump; making it incomplete.

Table 15 *Fixed in AOS-W 5.0.4.2*

Bug ID	Description
56747	A buffer leak caused by Wi-Fi encrypted jumbo frames which lead to a disruption in client connectivity and AP heartbeats has been fixed. Additionally, a new counter, called **WIFI Jumbo Denied**, has been added under `show datapath frame`.
43802 44696	A datapath timeout that occurs when global packet tracing is enabled has been fixed.
44973	An issue in which an AP did not always have the latest group key that the 802.1X module on the switch generates has been fixed. Now, whenever the switch sends out a un ica st key for any station connected to that AP, it also sends out the current multicast key. If the key the AP has, is different than what the switch is sending, then it is updated.

Table 15 *Fixed in AOS-W 5.0.4.2*

Bug ID	Description
46116	The TCP maximum segment size for TKIP tunnels has been reduced to better accommodate the WEPCRC length.
46747 50941 55236 58260	A Mesh AP crash due to an assert caused by a frame with no data after the 802.11 header has been fixed. The assert has been removed so such frames will simply be ignored.
48838	The **Clear Sessions on Role Update** Firewall setting now works correctly in the event of a RADIUS disconnect event.
49267 57767 58210 59495 59489 59388 56913 54133	An httpd process crash that prevented user from logging onto the network using Captive Portal has been fixed. This process crash was caused large amounts of auth memory corruption resulting httpd restarting to recover that memory.
49910 53933 56010 56193 57843 54695	An unexpected AP reboot caused by a memory issue that occurred when an AP in air monitor mode was upgraded has been fixed.
50027 50026	An ISAKMP module crash caused by a memory leak has been fixed.
51822	An AP reboot caused by a kernel page fault due to a corruption in mac_hash has been fixed.
52450 54880 54165 54323 58874	An issue in which APs connected to a local switch ignore association requests from clients after a reboot has been fixed.
52494	An auth module crash caused by a control process exception has been fixed.
52572	Honeywell Dolphin 9900 mobile scanners connected to Remote APs in bridge mode no longer intermittently lose their network connection.
52901	Clients that use an external captive portal to authenticate and connect to the network are assigned their correct authenticated user role.
53230	An unexpected switch reboot caused by a datapath timeout due a bad egress issue has been fixed.
53408	Clients connected to a virtual AP with an unconfigured VLAN will be able to reconnect to the network if the connection to between the switch and AP is lost and the AP reboots.
53443	If an AP loses power in the middle of a write operation, that AP's custom environment settings may be reset to factory default values. Starting with AOS-W 5.0.4.2, a remote AP only writes data to the flash memory when necessary, reducing the chance of AP errors if the AP loses power in the middle of a write operation.
54191	FTP data transfer and reuse of a stray session no longer triggers a race condition and datapath timeout exception.

Table 15 *Fixed in AOS-W 5.0.4.2*

Bug ID	Description
54194	Improvements to the PAPI timeout handler prevent memory errors that could trigger unwanted switch reboots.
54334	Improvements to SNMP tree update procedures allow new OIDs to return correct data.
54359	Throttling of management and authentication frames no longer prevent Polycom phones from connecting to the network.
54534	Clients using WEP encryption stay connected to the network while roaming, regardless of the timing between the client's association request and the processing of any data that has already been sent.
54847	APs configured with a Mexico or Vietnam country code no longer perform radar detection on non-DFS channels 36-48 and 149-165.
54912	Server derivation from a RADIUS server is no longer ignored and now works correctly and clients are now placed in the correct role.
55007	An unexpected switch reboot caused by a datapath timeout has been fixed.
55266	An unexpected switch reboot caused by an STM module crash has been fixed.
55334	The **tar logs** CLI command displays **netstat gethostby** and **lsof gethostby** error messages only if system logging is set to the DEBUG level.
55939	AP models OAW-AP124 and OAW-AP125 support the Croatia regulatory domain.
57145 57414 57596 58515 58996 56882	An unexpected switch reboot caused by a corruption in PAPI message leading to an invalid ingress upon downloading it to the datapath has been fixed.
58640	All OAW-AP92s and OAW-AP93s can now be successfully configured as remote APs.
59412 56561	A change has been made to AOS-W to prevent SOS crashes from incorrectly being interpreted as "User Pushed Reset." Previously, the reason was written from sbHeartbeat process once a SOS had crashed. However, in some cases, the user process was not run because the kernel became occupied with the SOS core dump and the reason for reboot was never written. Therefore, upon reboot, the reason is interpreted as "User pushed reset." Now, the reason for reboot is written once the message that a crash has occurred is received from SOS and before the SOS core dump begins.

Table 16 *Fixed in AOS-W 5.0.4.1*

Bug ID	Description
52892	A fix has been added to AOS-W to allow packets larger than 1468 bytes for clients using a virtual AP in bridge forwarding mode to pass on the OAW-AP68.

Table 17 *Fixed in AOS-W 5.0.4.0*

Bug ID	Description
36123	An XML query with usernames now works correctly.
36941 48318	ICMP requests are no longer being blocked on the local switch during config synchronization with the master switch.
42160 42877 43349	A unexpected switch reboot, accompanied by a fpapps crash, caused by a heap corruption in switchShowAllAccessGrpPrivate due to memory overrun by sprintf has been fixed.
43036 43391	The OAW-4604 switch no longer crashes when an AP is added behind a RAP.
43341	Switches now respond to DNS queries with their own IP addresses.
43386	The issue with the monitoring page not showing the correct information under Guest WLAN has been fixed.
43431	Client blacklisting now works correctly if the maximum authentication failures is configured to 2 or larger.
44109 52067 53119 51635	The WebUI now correctly displays that an upgrade from a local file is completed. Although the WebUI showed that the upgrade was not completed, it actually had been.
44309	APs are no longer susceptible to DoS attacks that are initiated by injecting malformed 802.11 authorization or association requests with an invalid station MAC address.
44837	The Layer 3 switch that connects the switch trunk port at the central site no longer shows up in the switch bridge as coming from a GRE tunnel. This fix prevents outages of remote devices on VLANs.
44942	Instead of displaying single bit ECC error in the error log, these errors are counted and displayed as a counter in `show memory debug`.
45158	A WebUI filtering issue based on the client MAC address has been fixed. Invalid page numbers no longer appear.
45719	An IP conflict with the 192.168.11.x range and the inability to bring up the OAW-RAP2WG in the 192.168.11.x network has been fixed.
45858	The option **Include Technical Support Information** is not selected by default when logs are downloaded.
45887 45572	The XML API now correctly sends location (Ethernet MAC) information.
46290	The `show provisioning-params` command no longer shows “invalid” display.
47553 47919	A switch STM crash caused by a control processor exception that occurred when the user count was high and most of users were not redirected to the captive portal page has been fixed.
47623	The false radar detection of an OAW-AP120 on JP3 DFS channels has been fixed.
48035	SNMP queries now displays user names up to 40 characters in length.

Table 17 *Fixed in AOS-W 5.0.4.0 (Continued)*

Bug ID	Description
48107 48802 38376	An issue in which the error log displays the message `SNMP agent timed out when sending a request to application WMS for object (object id)` and incorrectly reports the switch as down has been fixed.
48242	New TACACS log messages for management and tac-accounting users have been added.
48243	TACACS management log messages now contain a user name.
48244	A TACACS SNMP trap for failed management authentication has been added.
48836	The command `backup flash` no longer fails when executed on legacy switches.
48980	An auth module process crash resulting a switch reboot has been fixed.
49034 48995 50733 52040 52995 53669 55788	An AP crash accompanied by a break instruction in the kernel code has been fixed.
49271	You can now successfully delete a captive portal profile and user role without needing to restart the auth and httpd processes.
49576	When a server certificate is installed, switch now correctly responds to DNS query with the IP address specified by `ip cp-redirect-address` configuration.
49617	MAC OS 10.6.6 L2TP/IPSec VPN is successful with P1 rekey.
49728	An fpapps module crashes when `show interface port-channel` command is issued with lengthy configuration caused by a memory allocation issue has been fixed.
49736	A mobile IP process crash caused by a race condition has been fixed.
49741	When using provisioning@home, RAPs in the factory default configuration that are booted up using a provisioning image no longer receive a DHCP lease before PPPoE comes up.
49956	Logging has been added for SNMP traps fan failure in `raiseFanAlarm`. Additionally, a new logging function has been added to send a message when the fan returns to normal.
50094 52277	An issue in which APs did not come up after an upgrade due to mesh causing a DSCP value to be set in PAPI packets has been fixed.
50500	Client activity for wired client is now displayed correctly in the WebUI if the client is connected to RAP's ethernet port.
50631 52456 44958 52972 54571	An AP crash due to a kernel page fault caused by a stack corruption has been fixed.
50914	A connectivity issue in which a master switch could not contact a local switch has been fixed by having master retry sending the switch IP requests again and again using a 15 second timer.

Table 17 *Fixed in AOS-W 5.0.4.0 (Continued)*

Bug ID	Description
51406	Zero touch provisioning for RAPs now works correctly when PPPoE is configured. The service name value was not included when the RAP was configured through zero touch provisioning but it is not correctly included.
51408	The correct label name is now displayed on the Guest Provisioning print screen.
51553 51728 52750	An unexpected switch reboot caused by an STM module crash has been fixed.

51591	VIA is not supported on legacy switches. If you attempt to configure VIA on a legacy switch, you will receive the following error:
	`Error processing command 'aaa authentication via connection-profile "default" switch addr <ip-addr> internal-ip <ip-addr> desc "vpn" position 0':Error: VIA is not supported in this Platform`
	`Error processing command 'aaa authentication via connection-profile "default" auth-profile "default" position 0':Error: VIA is not supported in this Platform`

51888	The severity of unknown RADIUS attributes has been dropped from error to notice and MS-Link-Drop-Time-Limit attribute has been added to the dictionary.
51953 52114 52294 52619 52792	A datapath exception causing VIA switches to reboot regularly has been fixed.
51965 52714	Wireless clients now correctly receive IPv6 addresses due to changes to the way IPv6 policies are handled.
52092	When a client with a x.x.x.255 IP address pings its default gateway, the switch can properly learn the client's MAC address and reply to the ICMP requests, even if the configured VRRP Virtual IP falls in the same half of the subnet as the client.
52450	APs connected to a local switch no longer occasionally ignore association requests from clients after the AP reboots.
52592	Improvements to the global user table allow master switches in a master/backup topology to display promptly display user information in the output of the **show global-user-table** command.
52782 51877	A Remote AP can properly fail over to a 3G USB modem connected to the AP's USB port.
52898	Improvements to the OAW-RAP5WN USB host switch driver resolves registration errors seen when the remote AP comes up with a USB modem plugged into the AP's USB port.
52902 55698	Improvements to the user-miss counter fixes a situation where a falsely high user-miss threshold could cause IP frames to be dropped, incrementing the 'Frames dropped due to excessive user misses' counter.
53041	The Max ADP Time has been increased to 60 for AP Platforms (except OAW-RAP2WG and OAW-RAP5WN) to allow enough time for statically provisioned APs to complete ADP/DNS master discovery.
53218 53262	The auth module no longer fails to respond when the switch queries an LDAP server.
53267	EAP-termination now works correctly on the 620 switch.

Table 17 *Fixed in AOS-W 5.0.4.0 (Continued)*

Bug ID	Description
53438	An issue in which OAW-AP61s were rebooting every 3 to 5 minutes due to a kernel panic has been fixed by having the APs reject frames with lengths larger than the buffer size.
53494	The switch correctly processes NATed PPTP packets, allowing clients are able to establish a PPTP connection while connected to a switch.
53676	An OAW-AP105 no longer becomes stuck in the **down** state after bulk provisioning via the WebUI.
53835	OAW-AP124 and OAW-AP125 devices in A/B/G mode are now correctly assigned to DFS channels by ARM when configured to do so.
53953	Aggregated Medium Access Control Service Data Units (AMSDU) packets are no longer dropped by default. This change resolves an issue that prevented some Apple MAC OS X devices from passing TCP traffic.
54238	Clients using both machine authentication and user authentication will first be assigned a machine derived user role when the client passes machine authentication, then, once the client passes user authentication, will take the appropriate user-derived user role.
54333	Clients properly retain their server-derived user role when they roam between APs.
55000	An OAW-AP125 crash has been fixed by addressing an issue in which the AP incorrectly received a management frame for a virtual AP that is no longer present or a frame from a node which is no longer in the system.
55437	Clients no longer randomly lose connectivity and are now able to reconnect to a Dot1X (WPA2-AES) virtual AP bridge forwarding mode.
55536	This release supports a new Organizational Unique Identifier (OUI) 6c:f3:7f in Alcatel-Lucent product MAC addresses.

Chapter 3

Known Issues

The following sections of this chapter describe known issues and limitations for AOS-W 5.0.4.x:

Known Issues Identified in the Current Release

The table below describes the known issues and limitations identified in AOS-W 5.0.4.16:

Table 17 *Known Issues and Limitations*

Bug ID	Description
94066	**Symptom:** The stateful 802.1X authentication does not work in AOS-W 5.0.4.x. The clients are unable to authenticate when a port connected to the access point is configured as an **untrusted** port. **Scenario:** This issue occurs on OAW-4308 switches running AOS-W 5.0.4.x associated to a third-party access point such as D-Link. **Workaround:** Configure the port as a **trusted** port for the authentication to work.

Known Issues Identified in Previous Releases

The table below describes the known issues and limitations identified in previous versions of AOS-W 5.0.4.x:

Table 18 *Known Issues and Limitations*

Bug ID	Description
94511	**Symptom:** An OAW-S3 switch reboots and crashes frequently with the message **Reboot Cause: User pushed reset**. **Scenario:** This issue is observed in OAW-S3 switches running AOS-W 5.0.4.x in a master-local topology, where the switch acts as a master switch. **Workaround:** None.
94902	**Symptom:** A switch reboots and crashes with a message **Kernel Panic**. **Scenario:** This issue is observed in OAW-4504 switches running AOS-W 5.0.4.11 in a master-local topology, where the switch acts as a master switch. **Workaround:** None.
91301	**Symptom:** A standby master switch reboots unexpectedly. **Scenario:** Log files for the event indicate that a database corruption of the station table resulted in the WLAN Management System (WMS) process to crash on the standby master switch. This issue is observed in standby OAW-4324 switches running AOS-W 5.0.4.x in an active-standby topology. **Workaround:** None.

Table 18 *Known Issues and Limitations (Continued)*

Bug ID	Description
90081	**Symptom: Port Based Session ACL Hits** and **Port ACL Hits** are not present in the output of the **`show acl hits`** command, when 100+ entries are present in acl tables. **Scenario:** This issue occurs in switches running AOS-W 5.0.4.x. **Workaround:** Use the **`show datapath acl <acl-id>`** command to view the acl hits for the port session and port acl hits table, when 100+ acl entries are present.
45739	**Symptom:** Wired clients connected to an OAW-RAP5 or OAW-RAP2WG in tunnel mode are not able to complete 802.1X authentication. These clients are running Windows XP Service Pack 2 or Service Pack 3. Wireless clients do not experience this issue. **Workaround:** A global aaa authentication profile can prevent this.
46443	**Symptom:** Enabling Firewall TCP enforcement when IP mobility is enabled impacts Layer-3 mobility. **Workaround:** None
53357	**Symptom:** A captive portal page using custom HTML with no user or guest logon may fail to redirect the user. **Workaround:** Custom HTML can be used to resolve this issue.
54156 55217	**Symptom:** AOS-W does not support APs connected to Tunneled Node ports. **Workaround:** None
55046	**Symptom:** An unexpected local OAW-S3 switch reboot incorrectly reported as “User pushed reboot” but due to a bus/cache error has been identified. However, since BUS errors are printed in the console, console output can be captured to get this information. **Workaround:** None
54518	**Symptom:** Occasionally, mesh points randomly drop from the network and return after the subtending mesh portal is rebooted. Debugging has shown that the switch loses its ARP entry as broadcast ARP-REQ is being ignored by the mesh point. However, the APs are still reachable if there is a static ARP entry pointing at them. **Workaround:** Reboot the AP. Additionally, the mesh point will recover by itself by reforming the mesh link after PAPI times out. This recovery takes about 5 minutes with the default values for `system-profile: max-req-retries` and `system-profile: request retry interval`.
54640	**Symptom:** A User derivation rule with DHCP option 77 is not hit for wired clients that are directly connected to the switch. In this case, the role remains on what is configured in the Initial Role of the associated AAA profile. **Workaround:** None
54641	**Symptom:** The following configuration options are not available in the WebUI: • Outer VLAN configuration under the Virtual AP Profile • Q-in-Q configuration under ports • Global configuration of Q-in-Q **Workaround:** Configure QinQ using the CLI.

Table 18 *Known Issues and Limitations (Continued)*

Bug ID	Description
55299 55433	**Symptom:** AOS-W does not support the inner VLAN 0. Therefore, if you configure an outer VLAN that does not have an inner VLAN, the ingress packets will be dropped for that outer VLAN. If you have VRRP configured for local or master switches, those outer VLANs will not have corresponding inner VLANs. This can prevent VRRP from working when master redundancy is enabled on a non-AP VLAN and QinQ is enabled. **Workaround:** Use the encapsulation command to assign an inner VLAN for the switch's communication. The switch cannot use static ARP in this case. For example: The traffic between AP and switch's QinQ is [1000, 200]. The IKE, ping, IPSec, etc. run in VLAN 900. Manually assign an inner VLAN such as 100. Then the traffic will be QinQ encapsulated with [900, 100]. • In the interface configuration: `encapsulation dot1q 900 second-dot1q 100` • In QinQ acl configuration: `permit 900 100 none`
56666 66809	**Symptom:** When `dos-prevention` is enabled on a virtual AP, station entries might not be cleared from the switch and AP after a station leaves the network. **Workaround:** None
55860	**Symptom:** When provisioning an AP, a remote AP will not begin the PPPoE dialogue unless the master name is resolved first. A remote AP, with factory default settings, has the uplink port connected to a DS where a PPPoE server exists and DHCP is configured on the VLAN. When the remote AP comes up, it receives its IP address from DHCP while the PPPoE parameters are still not configured. If you configure the PPPoE details and master name, then the remote AP will still try to resolve the master name with the IP it received through DHCP (non-PPPoE). When the DNS resolution fails, the remote AP will not begin PPPoE and the remote AP will never come up. **Workaround:** Disconnect the remote AP's uplink while provisioning the remote AP.
55861	**Symptom:** When provisioning an AP, a remote AP (RAP) continues to send DNS packets to resolve the master-name with the wrong source IP even after the PPPoE IP is set up. **Workaround:** Disconnect the RAP uplink while provisioning the RAP.
55863	**Symptom:** When provisioning an AP, a remote AP (RAP) will attempt to receive an IP address from DHCP even when PPPoE parameters are configured. This can lead problems such as route tables having different interfaces or DNS packets coming out with the wrong source IP. **Workaround:** Disconnect the RAP uplink while provisioning the RAP.
55866	**Symptom:** When provisioning an AP, the remote AP (RAP) uses DHCP over the PPPoE link during RAP tunnel establishment. **Workaround:** Disconnect the RAP uplink while provisioning the RAP.
55879	**Symptom:** When provisioning an AP, you cannot configure a static IP address for a remote AP (RAP) while the uplink port is connected. If you configure a static IP for the RAP, once it successfully creates an IPSec tunnel the master it will begin sending a out DHCP discover packets and the RAP will fail to come up. **Workaround:** Disconnect the RAP uplink while provisioning the RAP.
59288 59434	**Symptom:** Wired 802.1X authentication does not work when mobility is enabled on the switch. During the 802.1X exchange, the switch enters a loop and continuously sends out EAP-ID requests, even after the client has responded with an EAP-ID response. **Workaround:** Turning off mobility allows you to avoid this issue.

Table 18 *Known Issues and Limitations (Continued)*

Bug ID	Description
60722 61100 57925 60846 64517 66118 66128 66185 66659 64526 61539 61196 67435 67670 67671 67673 67871 67872 67977 63460 65049 62111 66409 66136	**Symptom:** The Alcatel-Lucent OAW-4306GW switch crashes and unexpectedly reboot when the internal AP is enabled. **Workaround:** Disable the radio on the internal AP on the OAW-4306GW switch. To disable the radio for a specific AP, please follow the instructions provided in **""Known Issues Identified in Previous Releases" on page 25" on page 25**.
62358	**Symptom:** The following MIB OIDs show only legacy rates, and do not update with 802.11n (HT) rates, even for clients that support 802.11n. • 1.3.6.1.4.1.14823.2.2.1.1.2.2.1.8 (staTransmitRate) • 1.3.6.1.4.1.14823.2.2.1.1.2.2.1.9 (staReceiveRate) **Scenario:** This issue occurs on APs running AOS-W 5.0.3.2. These OIDs are not populated with 11n (HT) rates for 11n clients because they are updated with legacy rates only. **Workaround:** None
67276	**Symptom:** When a DHCP server gives out multiple default gateway IP addresses and one of the addresses is not reachable, associated APs will appear to be up but not reachable. **Workaround:** Remove the invalid default gateway (the unreachable IP) from the list of gateway IP addresses on the DHCP server.
67855	**Symptom:** A switch may not assign the correct bandwidth contract to a user when the user moves from one SSID to another; the user maintains the bandwidth contract from the previous SSID. **Workaround:** Delete the bandwidth contract in the new role and reapply it.
68035	**Symptom:** When site-to-site VPN is enabled between two switches, static routes are not removed from the routing table when site-to-site VPN goes down. This occurs when site-to-site VPN is enabled and a static route is added to the remote subnet with an IPsec map. **Workaround:** Delete the static route to the remote subnet.
68347	**Symptom:** Wireless clients cannot send packets on a virtual AP (VAP) that has derived more than 32 unique VLANs. Currently, AOS-W supports no more than 32 VLANs per VAP. **Workaround:** None
68650	**Symptom:** A remote AP (RAP) image upgrade from 5.0.4.x to a later release can take as long as 15 minutes. This occurs when the RAP is connected behind a NAT device and the NAT device's UDP session times out. **Workaround:** There is no workaround, but the RAP completes the upgrade in 15 minutes or less.
69829	**Symptom:** After upgrading to AOS-W 5.0.4.7, devices directly connected to port 22 on OAW-4324 switches regularly lose connectivity. This does not occur on ports 0 through 21. This issue is still under investigation. **Workaround:** None

Table 18 *Known Issues and Limitations (Continued)*

Bug ID	Description
73779	**Symptom:** The station and user tables on local switches show stale entries for users that aged out. **Scenario:** Stale entries for wireless users associated to a remote AP in bridge mode appeared on local switches running AOS-W 5.0.4.1 with control plane security disabled. This issue is primarily triggered by a remote AP rebootstrapping. **Workaround:** Remove individual stale entries by issuing the CLI command **aaa user delete ap-name <apname> ip <ip-addr>** , or reboot the remote AP during a maintenance window to clean up stale entries on that specific remote AP.
75514	**Symptom:** An internal switch module crashed, preventing CLI or WebUI access to the switch until the switch rebooted. **Scenario:** The issue is caused by a memory error triggered when the **show ap debug log ip-addr <ip-addr>** command is executed on a switch running AOS-W 5.0.3.2, and the switch tries to resolve the hostname/IP address. **Workaround:** None
76239	**Symptom:** VPN user entries do not properly age out of the user table. These user entries become stale and prevent new users with the same IP address from associating to the network. **Scenario:** The issue was identified on an OAW-4324 switch running AOS-W 5.0.4.5. **Workaround:** None.
77715	**Symptom**: An AP rebootstraps frequently when connected to a Power over Ethernet (PoE) port of an OAW-4306 Series switch and continually alternates between UP and DOWN states. This issue is under investigation. **Workaround**: Disable PoE on the port or move the AP to a non-PoE port on the switch.
78913	**Symptom**: The switch unexpectedly reboots. The log file for the event lists the reason for the reboot as **Kernel Panic**. **Scenario**: This issue occurs on a Supervisor Card I (OAW-S-1) switch running AOS-W 5.0.4.6. **Workaround**: Review L2 flood traffic in the network and apply appropriate bandwidth contracts.

Issues Under Investigation

The table below describes the issue under investigation identified in AOS-W 5.0.4.14:

Table 19 *Issues Under Investigation*

Bug ID	Description
92616	**Symptom:** Access Points reboot unexpectedly. The log files for the event listed the reason for the reboot as **Out of Memory**.

Alcatel-Lucent OAW-4306GW Internal AP

The Alcatel-Lucent OAW-4306GW switch reboots unexpectedly when the internal AP is enabled (bug 60722 and duplicates). To disable the internal AP, complete one of the following procedures:

In the CLI

1. Create a dot11g radio profile and disable the radio

```
(host) #configure terminal
(OAW-4306GW_switch) (config) # rf dot11g-radio-profile disable-radio
(OAW-4306GW_switch) (802.11g radio profile "disable-radio") #no radio-enable
(OAW-4306GW_switch) (802.11g radio profile "disable-radio") #exit
```

2. Apply the radio profile to a specific AP, then save the configuration.

```
(OAW-4306GW_switch) (config) #ap-name <ap-name>
(OAW-4306GW_switch) (AP name "<ap-name>") #dot11g-radio-profile disable-radio
(OAW-4306GW_switch) (AP name "<ap-name>") #end
(OAW-4306GW_switch) #write memory
```

In the WebUI

1. Navigate to **Configuration > Wireless > AP Configuration**. Select the **AP Specific** tab.
2. Click **Edit** by the AP for which you want to create a new RF management profile.
3. In the Profiles list, expand the **RF Management** menu, then select **802.11g radio profile**.
4. Click the **802.11g radio profile** drop-down list in the Profile Details window pane and select **NEW**.
5. Enter a name for your new 802.11g radio profile “disable-radio.”
6. Uncheck **Radio Enable** to disable the radio then click **Apply** to save your settings.

The following enhancements were added in previous versions of AOS-W 5.0.4.x:

Support for New Version of ETSI DFS standard

With the exception of OAW-RAP5WN and the OAW-AP120 Series APs, all supported APs will comply with version 1.6.1 or later of the ETSI DFS standard EN301893 when the system is upgraded to AOS-W 5.0.4.10.

The OAW-RAP5WN and OAW-AP120 Series APs can be upgraded to AOS-W 5.0.4.10 or later, but will not become compliant with the version 1.6.1 of the standard. RAP-5WN and AP-120 Series APs already installed in a network are allowed to remain compliant with the previous version of the standard, but any new devices added to the network after 12/31/2012 must comply with the version 1.6.1 or later wherever ETSI rules apply.

Regulatory Adjustments

The following changes impact new installations of OAW-AP124 and OAW-AP125 access points running AOS-W 5.0.4.13:

Table 20 *Channel/Domain Changes in this Release*

Country Domain	Regulatory Change
Changes for OAW-AP124/OAW-AP125 Access Points	
Kazakhstan and Dominican Republic	AOS-W now supports these country domains.
Australia and New Zealand	These country domains support all channels allowed by the FCC (including indoor, outdoor and DFS channels) . In previous releases, Australia and New Zealand used ETSI channels.
UAE	Removed support for channels 149-165.
Mexico	This domain requires Dynamic Frequency Selection (DFS) in all 802.11a channels. In previous releases, all 802.11a channels were open without DFS support.
Serbia	Added DFS support for channels 52-64 and100-140. These channels were not open in previous releases.
New Zealand, Puerto Rico, Columbia	Removed support for channels 120-128, because these channels were removed from the FCC list of allowed channels.

Country support and EIRP transmit power levels were updated in AOS-W 5.0.4.10 to reflect the latest regulatory status and test results.

QinQ (802.1ad)

AOS-W 5.0.4.0 introduces support of the QinQ Ethernet frame format. QinQ is an expansion of 802.1Q (VLAN tagging). The purpose of QinQ is to allow for an additional VLAN tag on the already tagged frame, creating a tag stack. A tag stack creates a mechanism for Internet Service Providers to encapsulate a customer's single-tagged 802.1Q traffic with a single tag, the final frame being a QinQ frame. The outer tag is used to identify and segregate traffic from different customers; the inner tag is preserved from the original frame.

Use the following command to set the QinQ mode on the switch. These commands require a switch reboot.

```
(switch) (config) #qinq mode {mixed-q-in-q | q-in-q}
  mixed-q-in-q Q-in-Q on some ports
  q-in-q Q-in-Q on all ports
```

Physical Interfaces

Use the following command to convert a port to a QinQ port:

```
(switch) (config) #interface {gigabitethernet | fastethernet} <slot><port>
(switch) (config-if) #qinq
```

Use the following commands to assign VLAN maps to the interfaces:

```
(switch) (config) #interface {gigabitethernet | fastethernet} <slot><port>
(switch) (config-if) #vlan-map-acl vmap1 in
```

Use the following command to set the inner-VLAN range for the special outer-VLAN on the Access Point (AP) side, so the broadcast packet to the AP can work:

```
(switch) (config) #interface {gigabitethernet | fastethernet} <slot><port>
(switch) (conf-if)# encapsulation dot1q vlan-id second-dot1q {vlan-id | vlan-id-vlan-id
[vlan-id-vlan-id]}
```

Port-Channel Interfaces

QinQ can also be configured on port-channel interfaces. Use the following command to convert a port-channel to a QinQ port-channel:

```
(switch) (config) #interface port-channel <id>
(switch) (config-if) #qinq
```

Use the following commands to assign VLAN maps to the interfaces:

```
(switch) (config) #interface port-channel <id>
(switch) (config-if) #vlan-map-acl vmap1 in
```

Use the following command to set the inner-VLAN range for the special outer-VLAN on the AP side, so the broadcast packet to the AP can work:

```
(switch) (config) #interface port-channel <id>
(switch) (conf-if)# encapsulation dot1q vlan-id second-dot1q {vlan-id | vlan-id-vlan-id
[vlan-id-vlan-id]}
```

Additional Commands

Use the following commands to configure the VLAN map ACL:

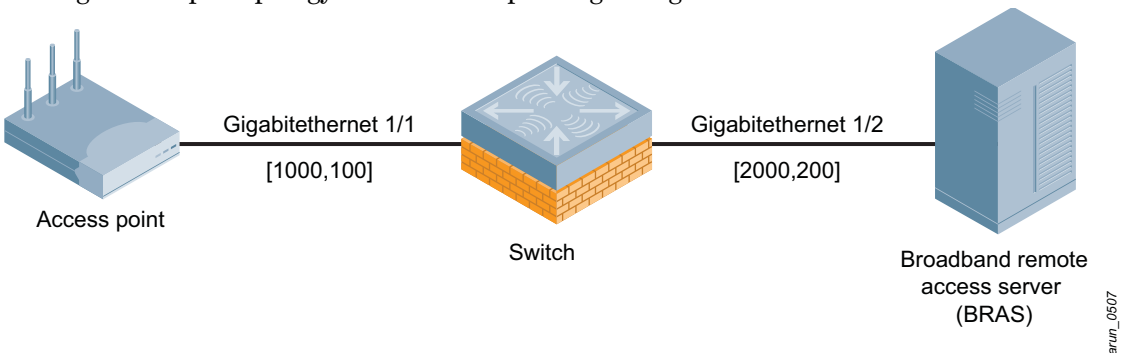
```
(switch) (config) #ip access-list qinq [name]
(switch) (config-qinq-name) #{permit|deny} <outer-vlan> <inner-vlans> <outer-vlan
action> <inner-vlan action>
Note: outer-vlan is a specific VLAN ID ranged from 1 to 4094
      inner-vlans is a VLAN range separated by "-"
      outer-vlan action is null, pop or swap <id>
      inner-vlan action is null, pop or swap <id>
```

Use the following command to set the outer-VLAN for the special virtual AP:

```
(switch) (config) (Virtual AP profile "vap") #
outer-vlan        List of VLANs to use for QinQ outer vlan in this virtual AP
```

Sample Topology and Configuration

The following is a sample topology and the corresponding configuration.




```
interface gigabitethernet 1/1
   switch mode trunk
   switch trunk allow vlan 1000 <-define the broadcast domain as outer vlan on AP side
   encapsulation dot1q 1000 second-dot1q 100 <-define the broadcast packet from switch to AP
            qinq <-enable QinQ in this port
vlan 1000
vlan 200
interface vlan 1000
   ip addr 192.168.1.1 255.255.255.0

ip dhcp pool AP
   network 192.168.1.0 255.255.255.0
service dhcp
ip access-list qinq bras
   permit 2000 200 pop <-define the vlan ACL used on BRAS side to pop the outer vlan
interface gigabitethernet 1/2
   switch mode trunk
   switch trunk allow vlan 200  <-define the broadcast domain as inner_vlan in BRAS side
   qinq                         <-enable QinQ
   vlan-map-acl bras in         <-apply the VLAN ACL to pop the outer_vlan in BRAS side

interface vlan 200
   ip addr 10.10.10.1 255.255.255.0

ip dhcp pool STA
   network 10.10.10.0 255.255.255.0

wlan ssid-profile aaa
   essid  aaa

wlan virtual-ap aaa
   outer-vlan 2000 <-define outer VLAN in virtual AP profile to set outer vlan to BRAS side
   vlan 200
   ssid-profile aaa

ap-group aaa
   virtual-ap aaa
```

New RAP Provisioning Image

A new remote AP provisioning image is introduced in AOS-W 5.0.4.0. This new image fixes bugs 49741 and 51406. For more information on these issues see Table 17 on page 20.

Updated MIB

The AOS-W MIB has been updated with the following new scalar objects (objects with a single instance), tabular objects (objects with multiple instances), MIB tables and traps. The scalar objects, tabular objects

and new tables can be monitored using a MIB Browser. The traps can be monitored using a trap receiver, or the `show snmp trap-queue` command in the AOS-W command-line interface.

New Scalar Objects in the AOS-W MIB

The following scalar objects were added to the AOS-W MIB to retrieve the switch system information. These objects are defined on node `wlsxSystemExtGroup`, appended to the end of this object group.

Table 21 *New Tabular Objects in the AOS-W MIB*

Object	Description
`wlsxSysExtHwVer`	Hardware version of the switch.
`wlsxSysExtSwVer`	Software version of the switch.
`wlsxSysExtSerialNumber`	The serial number of the switch.
`wlsxSysExtCpuUsedPercent`	The CPU used percent of the switch.
`wlsxSysExtMemoryUsedPercent`	The memory used percent of the switch.
`wlsxSysExtPacketLossPercent`	The packet loss percent of the switch.

New Tabular Objects in the AOS-W MIB

The AOS-W MIB now includes the following tabular objects, added to retrieve the statistics of the AP and the radio. All tabular objects introduced in AOS-W 5.0.4.14 are appended to the existing tables on node `wlsxWlanMIB`.

Table 22 *New Tabular Objects in the AOS-W MIB*

New Object	Definition	Table
`wlanAPHwVersion`	Hardware version of the AP	wlsxWlanAPTable
`wlanAPSwVersion`	Software version of the AP	wlsxWlanAPTable
`wlanAPBssidSnr`	The Signal Noise Ratio of this BSSID	wlsxWlanAPBssidTable
`wlanWarmReboots`	The number of warm starts of the AP	wlsxWlanAPTable
`wlanStaTransmitRateCode`	Transmit rate code with which the station is associated with this system. Unit values are in mbps.	wlsxWlanStationTable
`wlanAPWiredRxErrorPkts`	The number of error packets received from the switch on this BSSID	wlsxWlanAPStatsTable
`wlanAPRxErrorPkts`	The number of error packets received from stations on this BSSID.	wlsxWlanAPStatsTable

New Tables

The following tables will be added for SNMP to retrieve the statistics of the switch, the AP and the radio. Tables for AP and radio statistics will be added on node `wlsxWlanAccessPointStatsGroup`. A new

group `wlsxWlanSwitchStatsGroup`, is added on node `wlsxWlanStatsGroup` and collects switch-based statistics. All tables for switch-based statistics will be defined on this group.

Table 23 *New MIB Tables*

Table	Index(es)	Description
`wlsxWlanAPWiredStatsTable`	`wlanAPMacAddress`	The Wired statistics of all Access Points connected to the switch. Objects in this table are described in Table 24.
`wlsxWlanAPESSIDStatsTable`	`wlanAPMacAddress` `wlanESSID`	The ESSID statistics of all Access Points connected to the switch. Objects in this table are described in Table 25.
`wlsxWlanAPRadioStatsTable`	`wlanAPMacAddress` `wlanAPRadioNumber`	The Radio statistics of all Access Points connected to the switch. Objects in this table are described in Table 26.
`wlsxWlanESSIDStatsTable`	`wlanESSID`	The statistics of the whole network controlled by this switch. Objects in this table are described in Table 27.
`wlsxWlanEthStatsTable`	`ifIndex`	The statistics of all Ethernet ports of this switch. Objects in this table are described in Table 28.

`wlsxSSIDConfigTable`	`wlanAPMacAddress`
	`wlanAPRadioNumber`
	`wlanESSID`
	`wlanESSIDIndex`
		The configuration of the SSID. Objects in this table are described in Table 29.

`wlsxAPConfigTable`	`wlanAPMacAddress`	The configuration of the access point. Objects in this table are described in Table 30.

wlsxWlanAPWiredStatTable Objects

The following table lists the objects in the new MIB table `wlsxWlanAPWiredStatsTable`.

Table 24 *New Objects in table wlsxWlanAPWiredStatsTable*

Object	Description
`wlanAPWiredRxPkts`	The total packets received from the AP wired side.
`wlanAPWiredRxDroppedPkts`	The total dropped packets received from the AP wired side.
`wlanAPWiredRxBytes`	The total bytes of correct packets received from the AP wired side.
`wlanAPWiredTxBytes`	The total bytes transmitted from the AP wired side.
`wlanAPWiredRxRate`	The data rate (kbyte/s) received from AP wired side in sampling interval.
`wlanAPWiredTxRate`	The data rate (kbyte/s) transmitted from AP wired side in sampling interval.

wlsxWlanAPESSIDStatsTable Objects

The following table lists the objects in the new MIB table `wlsxWlanAPESSIDStatsTable`.

Table 25 *New Objects in table wlsxWlanAPESSIDStatsTable*

Object	Description
`wlanAPESSIDWirelessRxBytes`	The total bytes of correct packets received from the AP ESSID wireless side.
`wlanAPESSIDWirelessTxBytes`	The total bytes transmitted from the AP ESSID wireless side.
`wlanAPESSIDWiredRxBytes`	The total bytes of correct packets received from the AP ESSID wired side.
`wlanAPESSIDWiredTxBytes`	The total bytes transmitted from the AP ESSID wired side.

wlsxWlanAPRadioStatsTable Objects

The following table lists the objects in the new MIB table `wlsxWlanAPRadioStatsTable`.

Table 26 *New Objects in table wlsxWlanAPRadioStatsTable*

Object	Description
`wlanAPRadioRxPkts`	The total packets transmitted from the AP radio wireless side.
`wlanAPRadioRxBytes`	The total correct bytes received from the AP radio wireless side.
`wlanAPRadioTxPkts`	The total packets transmitted from the AP radio wireless side.
`wlanAPRadioTxBytes`	The total bytes transmitted from the AP radio wireless side.
`wlanAPRadioTxDroppedPkts`	The dropped packets transmitted from the AP radio wireless side.
`wlanAPRadioTxErrorPkts`	The error packets transmitted from the AP radio wireless side.
`wlanAPRadioRxRate`	The data rate (kbyte/s) received from AP radio wireless side in sampling interval.
`wlanAPRadioTxRate`	The data rate (kbyte/s) transmitted from AP radio wireless side in sampling interval.
`wlanApRadioAssocReqCount`	The times of associate request on this radio.
`wlanApRadioAssocReqSuccCount`	The times of successful associate request on this radio.
`wlanApRadioReAssocReqCount`	The times of re-associate request on this radio.
`wlanApRadioReAssocReqSuccCount`	The times of successful re-associate request on this radio.
`wlanAPRadioStationDuration`	The total duration occupied by the user on this radio.
`wlanAPRadioAssocSuccPercent`	The Association Success Percent on this radio.

wlsxWlanESSIDStatsTable Objects

The following table lists the objects in the new MIB table `wlsxWlanESSIDStatsTable`.

Table 27 *New Objects in table wlsxWlanESSIDStatsTable*

Object	Description
`wlanESSIDRxPkts`	The total number of packets on the ESSID uplink channel of wireless side.
`wlanESSIDRxDroppedPkts`	The total number of dropped packets on the ESSID uplink channel of wireless side.
`wlanESSIDRxRetryPkts`	The total number of re-transmission packets on the ESSID uplink channel of wireless side.
`wlanESSIDWiredTxBytes`	The total number of bytes on the ESSID downlink channel of wireless side.

wlsxWlanEthStatsTable Objects

The following table lists the objects in the new MIB table `wlsxWlanEthStatsTable`.

Table 28 *New Objects in table wlsxWlanEthStatsTable*

Object	Description
`wlanEthRxRate`	The data rate received from the Ethernet port in sampling interval, unit is kbyte/s.
`wlanEthTxRate`	The data rate transmitted from the Ethernet port in sampling interval, unit is kbyte/s.

wlsxSSIDConfigTable Objects

The following table lists the objects in the new MIB table `wlsxSSIDConfigTable`.

Table 29 *New Objects in table wlsxSSIDConfigTable*

Object	Description
`wlanESSIDIndex`	The index of ESSID, value range from 1 to 16.
`wlanSSIDConfigHideSSID`	This attribute indicates if SSID is hidden or not.
`wlanSSIDConfigNumStaAllowed`	The maximum number of stations that are allowed to access into the network.
`wlanSSIDConfigWmmBeDscp`	The QoS priority of best-effort service.
`wlanSSIDConfigWmmBkDscp`	The QoS priority of background service.
`wlanSSIDConfigWmmViDscp`	The QoS priority of video service.
`wlanSSIDConfigWmmVoDscp`	The QoS priority of voice service.

wlsxAPConfigTable Objects

The following table lists the objects in the new MIB table `wlsxSSIDConfigTable`.

Table 30 *New Objects in table wlsxAPConfigTable*

Object	Description
`wlanAPConfigNetmask`	The netmask of AP IP Address.
`wlanAPConfigGateway`	The gateway of the AP.

New Traps

The following traps were added to the node `wlsxTrapsGroup` in the Alcatel-Lucent SNMP MIB. These traps will be generated by the switch or AP. A new trap object, `wlsxTrapCount`, represents the number of times of the trap occurred, and was added on node `wlsxTrapObjectsGroup`.

Following table describes the new traps and objects contained in the new traps when they are sent.

Table 31 *New MIB Traps*

Trap	Objects in Traps	Description

`wlsxAPNumUpgradeFailure`	`wlsxTrapAPMacAddress`
	`wlsxTrapAPLocation`
	`wlsxTrapCount`
		A trap which indicates the number of upgrade failure of an Access Point. This trap is generated by the Access Point.

`wlsxAPNumWarmStarts`	`wlsxTrapAPMacAddress`
	`wlsxTrapAPLocation`
	`wlsxTrapAPIpAddress`
	`wlsxTrapCount`
		A trap which indicates the number of warm starts of an Access Point. This trap is generated by the switch.

`wlsxAPNumColdStarts`	`wlsxTrapAPMacAddress`
	`wlsxTrapAPLocation`
	`wlsxTrapAPIpAddress`
	`wlsxTrapCount`
		A trap which indicates the number of cold starts of an Access Point. This trap is generated by the switch.

`wlsxAPNumDown`	`wlsxTrapAPMacAddress`
	`wlsxTrapAPLocation`
	`wlsxTrapAPIpAddress`
	`wlsxTrapCount`
		A trap which indicates the number of down alarms of an Access Point. This trap is generated by the switch.

`wlsxAPNumRadioDown`	`wlsxTrapAPMacAddress`
	`wlsxTrapAPLocation`
	`wlsxTrapAPIpAddress`
	`wlsxTrapCount`
		A trap which indicates the number of radio down alarms of an Access Point. This trap is generated by the switch.

`wlsxNumClockSyncErrors`	`wlsxTrapCount`	A trap which indicates the total number of clock sync errors between the switch and Access Points. This trap is generated by the switch.
`wlsxNumColdStart`	`wlsxTrapCount`	A trap which indicates the number of cold-starts of the switch. This trap is generated by the switch. Note: This trap is generated only after SP licenses are installed.

Table 31 *New MIB Traps*

Trap	Objects in Traps	Description
wlsxNumWarmStart	wlsxTrapCount	A trap which indicates the number of warm-starts of the switch. This trap is generated by the switch. Note: This trap is generated only after SP licenses are installed.

The section below shows the output of these traps as displayed in the `show snmp trap-queue` CLI command:

- wlsxAPNumUpgradeFailure

  ```
  2011-01-05 05:58:00 Access point 00:24:6c:c7:e0:70 with name 00:24:6c:c7:e0:70
  failed to upgrade 8 times
  ```

- wlsxAPNumWarmStarts

  ```
  2011-01-05 05:58:00 Access point 00:24:6c:c7:e0:70 with name 00:24:6c:c7:e0:70 and IP
  address 10.0.0.254 warm-started 20 time(s)
  ```

- wlsxAPNumColdStarts

  ```
  2011-01-05 05:58:00 Access point 00:24:6c:c7:e0:70 with Name 00:24:6c:c7:e0:70 and IP
  address 10.0.0.254 cold-started 20 time(s)
  ```

- wlsxAPNumDown

  ```
  2011-01-05 05:58:00 Access point 00:24:6c:c7:e0:70 with Name 00:24:6c:c7:e0:70 and IP
  address 10.0.0.254 has been down 20 time(s)
  ```

- wlsxAPNumRadioDown

  ```
  2011-01-05 05:58:00 Access point 00:24:6c:c7:e0:70 with Name 00:24:6c:c7:e0:70 and IP
  address 10.0.0.254 turned off radio 6 time(s)
  ```

- wlsxNumClockSyncErrors

  ```
  2011-01-05 05:58:00 The switch had clock sync error with access points 20 time(s)
  ```

- wlsxNumColdStart

  ```
  2011-01-05 05:58:00 The switch switch cold-started for 20 time(s)
  ```

- wlsxNumWarmStart

  ```
  2011-01-05 05:58:00 The switch switch warm-started for 20 time(s)
  ```

The traps `wlsxNumColdStart` and `wlsxNumWarmStart` are generated only after service provider AP licenses are installed.

Chapter 5

Upgrade Procedures

This chapter details software and hardware upgrade procedures. Best practices recommend that you schedule a maintenance window when upgrading your switches.

Read all the information in this chapter before upgrading your switches.

Topics in this chapter include:

All versions assume that you have upgraded to the most recent version as posted on the Alcatel-Lucent download site. For instance, 3.3.x assumes you have upgraded to the most recent version of 3.3.

Important Points to Remember

Upgrading your Alcatel-Lucent infrastructure can be confusing. To optimize your upgrade procedure, take the actions listed below to ensure your upgrade is successful. You should create a permanent list of this information for future use.

- Best practices recommend upgrading during a maintenance window. This will limit the troubleshooting variables.
- Verify your current AOS-W version (execute the **show version** or the **show image version** command).
- Verify which services you are using for each switch (for example, Employee Wireless, Guest Access, Remote AP, Wireless Voice).
- Verify the exact number of access points (APs) you have assigned to each switch.
- List which method each AP uses to discover each switch (DNS, DHCP Option, broadcast), and verify that those methods are operating as expected.
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- List the devices in your infrastructure used to provide your wireless users with connectivity (Core switches, radius servers, DHCP servers, firewall, for example).

Technical Upgrading Best Practices

- Know your topology. The most important path is the connectivity between your APs and their switches. Connectivity issues will interfere with a successful upgrade. You must have the ability to test and make connectivity changes (routing, switching, DHCP, authentication) to ensure your traffic path is functioning.
- Avoid combining a software upgrade with other upgrades; this will limit your troubleshooting variables.
- Avoid making configuration changes during your upgrade.
- Notify your community, well in advance, of your intention to upgrade.
- Verify that all of your switches are running the same software version in a master-local relationship. The same software version assures consistent behavior in a multi-switch environment.
- Use FTP to upload software images to the switch. FTP is much faster than TFTP and also offers more resilience over slower links.

If you must use TFTP, ensure that your TFTP servers can send more then 30 MB of data.

- Always upgrade the non-boot partition first. If something happens during upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.

Basic Upgrade Sequence

Testing your clients and ensuring performance and connectivity is probably the most time-consuming part of the upgrade. Best practices recommends that you enlist users in different locations to assist with the validation before you begin the upgrade. The list below is an overview of the upgrade and validation procedures.

If you manage your switches via the AirWave Wireless Management Suite, the AirWave upgrade process automates most of these steps.

1. Upload the same version of the new software image onto all switches.
2. Reboot all switches simultaneously.
3. Execute the **ping -t** command to verify all your switches are up after the reboot.
4. Open a Secure Shell session (SSH) on your Master Switch.
5. Execute the **show ap database** command to determine if your APs are up and ready to accept clients.
6. Execute the **show ap active** to view the up and running APs.
7. Cycle between step 5 and step 6 until a sufficient amount of APs are confirmed up and running.

   The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table** <*access point ip address*> command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.
8. Verify that the number of access points and clients are what you would expect.
9. Test a different type of client for each access method (802.1X, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.

Managing Flash Memory

All Alcatel-Lucent switches store critical configuration data on an onboard compact flash memory module. To maintain the reliability of your WLAN network, Alcatel-Lucent recommends the following compact flash memory best practices:

- Do not exceed the size of the flash file system. For example, loading multiple large building JPEGs for RF Plan can consume flash space quickly.

  Warning messages alert you that the file system is running out of space if there is a write attempt to flash and 5 MB or less of space remains.

Other tasks which are sensitive to insufficient flash file system space include:

- DHCP lease and renew information is stored in flash. If the file system is full, DHCP addresses can not be distributed or renewed.
- If a switch encounters a problem and it needs to write a log file, it will not be able to do so if the file system is full and critical troubleshooting information will be lost

In certain situations, a reboot or a shutdown could cause the switch to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before rebooting.

Before you upgrade

You should ensure the following before installing a new image on the switch:

- Make sure you have at least 10 MB of free compact flash space (**show storage** command).
- Run the **tar crash** command to ensure there are no "process died" files clogging up memory and FTP/TFTP the files to another storage device.
- Remove all unnecessary saved files from flash (**delete filename** command).

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage facility. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Customer captive portal pages
- Customer x.509 certificates

Backup and Restore Compact Flash on the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the switch:

1. Navigate to the **Maintenance > File > Backup Flash** page.
2. Click **Create Backup** to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz.
3. Click **Copy Backup** to copy the file to an external server.

You can later copy the backup file from the external server to the Compact Flash file system by navigating to the **Maintenance > File > Copy Files** page.

4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Backup and Restore Compact Flash on the CLI

The following steps describe the back up and restore procedure for the entire Compact Flash file system using the switch's command line:

1. Enter **enable** mode in the CLI on the switch. Use the **backup** command to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz:

```
(host) # backup flash
Please wait while we tar relevant files from flash...
Please wait while we compress the tar file...
Checking for free space on flash...
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
```

2. Use the **copy** command to transfer the backup flash file to an external server:

```
(host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
<remote directory>
```

   You can later transfer the backup flash file from the external server to the Compact Flash file system with the copy command:

```
(host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
```

3. Use the **restore** command to untar and extract the *flashbackup.tar.gz* file to the Compact Flash file system:

```
(host) # restore flash
```

License Mapping

License consolidation and even renaming of licenses occur over time. Figure 2 is an up-to-date illustration of the consolidated licenses effective with this release.

Licensing Change History

The following changes and/or consolidations were made to the AOS-W licensing.

AOS-W 5.0

- MAP was merged into base AOS-W
- VPN was merged into base AOS-W
- RAP was merged into AP license
- PEF (user basis) was converted to PEFNG (AP basis) with AOS-W 5.0

AOS-W 3.4.1

- VOC was merged into PEF. This merge happened with AOS-W 3.4.1
- IMP was merged into base AOS-W

AOS-W 3.4.0

- ESI was merged into PEF

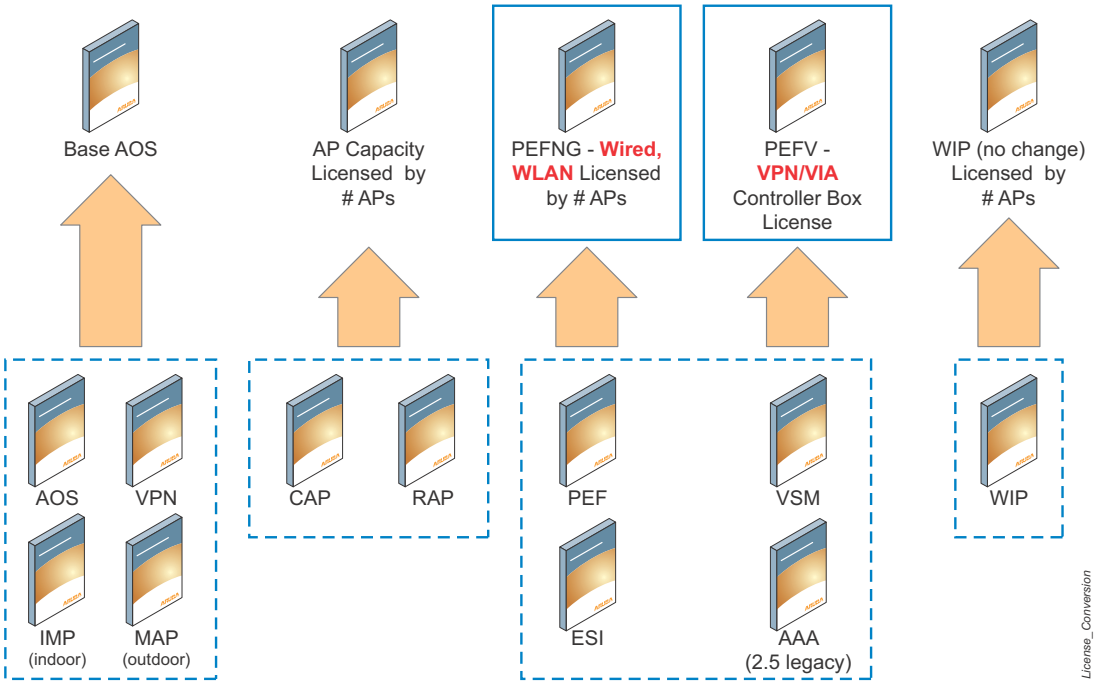
AOS-W Legacy and End-of-Life

- AAA was merged into ESI with the release of AOS-W 2.5.3.
- CIM is End-of-life

NOTE

Releases older than AOS-W 2.5.4 have reached End-of-Life status.

Figure 2 *License Consolidation*



Upgrading from 3.4.x to 5.0

Read all the following information before you upgrade to the latest version of AOS-W. If you are upgrading from a version earlier than 3.4.x, see "Upgrading from 3.3.x to 5.0" on page 48 or "Upgrading from 2.5.x to 3.3.x to 5.0" on page 49.

Caveats

Before upgrading to AOS-W 5.0 take note of these known upgrade caveats.

- If you have occasion to downgrade to a prior version, and your current AOS-W 5.0 configuration has control plane security (CPsec) enabled, you must disable control plane security before you downgrade.

  For more information on configuring control plane security and auto-certificate provisioning, refer to the *AOS-W 5.0 User Guide*.

Load New Licenses

Before you upgrade to AOS-W 5.0, assess your software license requirements and load any new or expanded licenses you require prior to upgrading to AOS-W 5.0.

Software licenses in AOS-W 5.0 are consolidated and in some instances license names and modules are renamed to more accurately represent the modules supported by the licenses (see Figure 2).

For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the user guide.

If you need to downgrade to AOS-W 3.4.x, the previous licenses will be restored. However, once you upgrade again to AOS-W 5.0 the licenses will no longer revert should you need to downgrade again.

Upgrading to 5.0.4

Read all the following information before you upgrade to AOS-W 5.0.4.11.

- "Save your Configuration" on page 46
- "Install AOS-W 5.0.4.16" on page 46

Save your Configuration

Before upgrading, save your configuration and back up your switches data files (see "Managing Flash Memory" on page 43). Saving your configuration saves the **admin** and **enable** passwords in the proper format.

Saving the Configuration on the WebUI

1. Click the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the screen.

Saving the Configuration on the CLI

Enter the following command in enable or config mode:

```
(host) #write memory
```

Install AOS-W 5.0.4.16

Download the latest software image from the Alcatel-Lucent Customer Support website.

When upgrading the software in a multi-switch network (one that uses two or more Alcatel-Lucent switches), special care must be taken to upgrade all the switches in the network and to upgrade them in the proper sequence. (See "Upgrading in a Multi-Switch Network" on page 49.)

Install AOS-W 5.0.4.16 on the WebUI

The following steps describe how to install the AOS-W software image from a PC or workstation using the Web User Interface (WebUI) on the switch. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Upload the new software image to a PC or workstation on your network.
2. Log in to the WebUI from the PC or workstation.
3. Navigate to the **Maintenance > Switch > Image Management** page. Select the Upload Local File option, then click the **Browse** button to navigate to the image file on your PC or workstation.

4. Determine which memory partition will be used to hold the new software image. Best practices is to load the new image onto the backup partition. To see the current boot partition, navigate to the **Maintenance > Switch > Boot Parameters** page.
5. Select **Yes** for Reboot Switch After Upgrade.
6. Click **Upgrade**.
7. When the software image is uploaded to the switch, a popup appears. Click **OK** in the popup window. The boot process starts automatically within a few seconds (unless you cancel it).
8. When the boot process is complete, log in to the WebUI and navigate to the **Monitoring > Switch > Switch Summary** page to verify the upgrade, including country code. The Country field displays the country code configured on the switch.

Install AOS-W 5.0.4.16 on the CLI

The following steps describe how to install the AOS-W software image using the CLI on the switch. You need a FTP/TFTP server on the same network switch you are upgrading.

1. Upload the new software image to your FTP/TFTP server on your network.
2. Execute the ping command to verify the network connection from the target switch to the FTP/TFTP server:

   ```
   (host) # ping <ftphost>
   ```

   or

   ```
   (host) # ping <tftphost>
   ```

A valid IP route must exist between the FTP/TFTP server and the switch. A placeholder file with the destination filename and proper write permissions must exist on the FTP/TFTP server prior to executing the **copy** command.

3. Determine which partition d to load the new software image. Use the following command to check the partitions:

   ```
   #show image version
   -----------------------------------
   Partition : 0:0 (/dev/hda1) **Default boot**
   Software Version : AOS-W 5.0.2.0 (Digitally Signed - Production Build)
   Build number : 20219
   Label : 20219
   Built on : 2009-05-11 20:51:46 PST
   -----------------------------------
   Partition : 0:1 (/dev/hda2)
   /dev/hda2: Image not present
   ```

   Best practices is to load the new image onto the backup partition (the non-boot partition). In the above example, partition 0 is the boot partition. Partition 1 is empty (image not present) and can be used to load the new software.
4. Use the **copy** command to load the new image onto the switch:

   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```

   or

   ```
   host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```

When using the **copy** command to load a software image, the specified partition automatically becomes active (default boot partition) the next time the switch is rebooted. There is no need to manually select the partition.

5. Execute the **show image version** command to verify the new image is loaded:

   ```
   (host) #show image version
   ```

6. Reboot the switch:

```
(host) # reload
```

7. Execute the **show version** command to verify the reload and upgrade is complete.

```
Compiled on 2014-05-23 at 17:48:41 PST (build 41905) by p4build
```

Upgrading from 3.3.x to 5.0

The following steps describe how to install the AOS-W software image from a PC or workstation using the Web User Interface (WebUI) on the switch. You can also install the software image from a FTP/TFTP server using the same WebUI page.

Upgrading on the WebUI

1. Upload the new software image to a PC or workstation on your network.
2. Log in to the WebUI from the PC or workstation.
3. Navigate to the **Maintenance > Switch > Image Management** page. Select the Upload Local File option, then click the **Browse** button to navigate to the image file on your PC or workstation.
4. Determine which memory partition will be used to hold the new software image. Best practices is to load the new image into the backup partition. To view the current boot partition, navigate to the **Maintenance > Switch > Boot Parameters** page.
5. Select **Yes** for Reboot Switch After Upgrade.
6. Click **Upgrade**.
7. When the software image is uploaded to the switch, a popup appears. Click **OK** in the popup window. The boot process starts automatically within a few seconds (unless you cancel it).
8. When the boot process is complete, log in to the WebUI and navigate to the **Monitoring > Switch > Switch Summary** page to verify the upgrade, including country code. The Country field displays the country code configured on the switch.

Upgrading on the CLI

The following steps describe how to install the AOS-W software image using the CLI on the switch. You need a FTP/TFTP server on the same network switch you are upgrading.

1. Upload the new software image to your FTP/TFTP server on your network.
2. Execute the ping command to verify the network connection from the target switch to the FTP/TFTP server:

```
(host) # ping <ftphost>
```

or

```
(host) # ping <tftphost>
```

A valid IP route must exist between the FTP/TFTP server and the switch. A placeholder file with the destination filename and proper write permissions must exist on the FTP/TFTP server prior to executing the **copy** command.

3. Determine which partition to load the new software image. Best practices are to load the new image onto the backup partition (the non-boot partition). In the above example, partition 0 is the boot partition. Partition 1 is empty (image not present) and can be used to load the new software.
4. Use the **copy** command to load the new image onto the switch:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
```

or

```
host) # copy tftp: <tftphost> <image filename> system: partition 1
```

When using the **copy** command to load a software image, the specified partition automatically becomes active (default boot partition) the next time the switch is rebooted. There is no need to manually select the partition.

5. Verify that the new image is loaded:

```
(host) # show image version
```

6. Reboot the switch:

```
(host) # reload
```

7. When the boot process is complete, use the **show version** command to verify the upgrade.

Upgrading from 2.5.x to 3.3.x to 5.0

Upgrading from AOS-W 2.5.x to AOS-W 5.0 requires an "upgrade hop". That is, you must upgrade from AOS-W 2.5.x to AOS-W 3.3.x first and then from AOS-W 3.3.x to AOS-W 5.0.

Once you have completed the upgrade to the latest version of 3.3.x, then follow the steps in "Upgrading from 3.3.x to 5.0" on page 48 to complete your last "upgrade hop".

Upgrading in a Multi-Switch Network

In a multi-switch network (a network with two or more Alcatel-Lucent switches), special care must be taken to upgrade all switches based on the switch type (master or local). Be sure to back up all switches being upgraded, as described in "Backing up Critical Data" on page 43.

For proper operation, all switches in the network must be upgraded with the same version of AOS-W software. For redundant (VRRP) environments, the switches should be the same model.

To upgrade an existing multi-switch system to AOS-W 5.0:

1. Load the software image onto all switches (including redundant master switches).
2. If all the switches cannot be upgraded with the same software image and reloaded simultaneously, use the following guidelines:
   a. Remove the link between the master and local mobility switches.
   b. Upgrade the software image, then reload the master and local switches one by one.
   c. Verify that the master and all local switches are upgraded properly.
   d. Connect the link between the master and local switches.

Pre-shared Key for Inter-Switch Communication

A pre-shared key (PSK) is used to create IPsec tunnels between a master and backup master switches and between master and local switches. These inter-switch IPsec tunnels carry management traffic such as mobility, configuration, and master-local information.

An inter-switch IP Sec tunnel can be used to route data between networks attached to the switches. To route traffic, configure a static route on each switch specifying the destination network and the name of the IP Sec tunnel.

There is a default PSK to allow inter-switch communications, however, for security you need to configure a unique PSK for each switch pair. You can use either the WebUI or CLI to configure a 6-64 character PSK on master and local switches.

CAUTION

Do not use the default global PSK on a master or standalone switch. If you have a multi-switch network then configure the local switches to match the new IP Sec PSK key on the master switch. Leaving the PSK set to the default value exposes the IP Sec channel to serious risk, therefore you should always configure a unique PSK for each switch pair.

Downgrading after an Upgrade

If necessary, you can return to your previous version of AOS-W.

WARNING

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. Any new entries that were created in the latest version of AOS-W will be lost after downgrade (this warning does not apply to upgrades from 3.4.x to 5.0),

Before you reboot the switch with the pre-upgrade software version, you must perform the following steps:

1. Verify that Disable Control Plane Security (CPSec) is disabled.
2. Set the switch to boot with the previously-saved pre-upgrade configuration file.
3. Set the switch to boot from the system partition that contains the pre-upgrade image file.

NOTE

When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file that will be used on the next switch reload. An error message displays if a system boot parameters are set for incompatible image and configuration files.

After downgrading the software on the switch:

- Restore your configuration from your pre-upgrade configuration back up stored on your flash file. Do not restore the flash file system from the latest version of the backup file.
- You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in the latest version of AOS-W, the changes will not appear in RF Plan in the downgraded AOS-W version.
- If you installed any certificates while running the latest version of AOS-W, you need to reinstall the certificates in the downgraded AOS-W version.

The following sections describe how to use the WebUI or CLI to downgrade the software on the switch.

Be sure to back up your switch before reverting the OS.

CAUTION

When reverting the switch software, whenever possible use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Downgrading on the WebUI

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the switch by navigating to the **Maintenance > File > Copy Files** page.
   a. For Source Selection, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
   b. For Destination Selection, enter a filename (other than default.cfg) for Flash File System.

2. Set the switch to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Switch > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the Configuration File menu.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Switch > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition):
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Switch > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Switch > Reboot Switch** page. Click **Continue**. The switch reboots after the countdown period.
6. When the boot process is complete, verify that the switch is using the correct software by navigating to the **Maintenance > Switch > Image Management** page.

Downgrading on the CLI

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the switch:

   ```
   (host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
   ```

   or

   ```
   (host) # copy tftp: <tftphost> <image filename> system: partition 1
   ```
2. Set the switch to boot with your pre-upgrade configuration file.

   ```
   # boot config-file <backup configuration filename>
   ```
3. Execute the **show image version** command to view the partition on which your previous software image is stored.

You cannot load a new image into the active system partition (the default boot).

4. Set the backup system partition as the new boot partition:

   ```
   # boot system partition 0
   ```
5. Reboot the switch:

   ```
   # reload
   ```
6. When the boot process is complete, verify that the switch is using the correct software:

   ```
   # show image version
   ```

Switch Migration

This section outlines the steps involved in migrating from an Alcatel-Lucent PPC switch environment to MIPS switch environment. These steps takes into consideration the common Alcatel-Lucent WLAN switch environment. You must have an operational PPC switch in the environment when migrating to a new switch. The switches are classified as:

- MIPS Switches—OAW-S3 and OAW-4306 Series

- PPC Switches—OAW-4302, OAW-4308, OAW-4324, 5000, and SC1/SC2 Migration instructions include:

Use this procedure to upgrade from one switch model to another. Take care to ensure that the new switch has equal or greater capacity than the switch you are replacing.

- "Single Switch Environment" on page 52
- "Multiple Master Switch Environment" on page 52
- "Master/Local Switch Environment" on page 52

Single Switch Environment

A single switch environment is one active switch, or one master switch that may have standby master switch that backs up the master switch.

- Replacing the standby switch—Does not require downtime
- Replacing the master switch—Requires downtime

Multiple Master Switch Environment

An all master environment is considered an extension of the single master switch. You can back up the master switches with a standby switch. In an all master switch deployment, each master switch is migrated as if it were in a standalone single switch environment.

For every master-standby switch pair

- Replacing the standby switch—Does not require downtime
- Replacing the master switch—Requires downtime

Master/Local Switch Environment

In a master/local environment, replace the master switch first and then replace the local switches.

- Replacing the local standbys (when present)
- Replacing local switches—one switch at a time

Before You Start

You must have:

- Administrative access to the switch via the network
- Administrative access to the switch via the switch's serial port
- Pre-configured FTP/TFTP server that can be reached from the switch
- Alcatel-Lucent serial cable
- The AOS-W version (same as the rest of the network)

Basic Migration Steps

1. Upgrade your network to the newer image to ensure that the image on the newer switches match the image on the rest of the switches in your network.
2. Backup the switch data from the PPC switch.
3. Physically swap the hardware (for example, mounting, cabling, power).
4. Initialize the new switch.
5. Install the backed up data onto the new switch.
6. Test the new setup.

Before You Call Technical Support

Before you place a call to Technical Support, please follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Alcatel-Lucent switch with IP addresses and Interface numbers if possible).
2. Provide the switch logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
3. Provide the syslog file of the switch at the time of the problem.

   Alcatel-Lucent strongly recommends that you consider adding a syslog server if you do not already have one to capture from the switch.
4. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have:
   - an outage in a network that worked in the past.
   - a network configuration that has never worked.
   - a brand new installation.
5. Let the support person know if there are any recent changes in your network (external to the Alcatel-Lucent switch) or any recent changes to your switch and/or AP configuration.
6. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred.
8. If the problem is reproducible, list the exact steps taken to recreate the problem.
9. Provide any wired or wireless sniffer traces taken during the time of the problem.
10. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
11. Provide the switch site access information, if possible.